SPECIFICATION

TITLE OF INVENTION

METHOD AND APPARATUS FOR CRYPTOGRAPHICALLY PROCESSING DATA

FIELD OF THE INVENTION

[0001] The present invention relates to cryptography and cryptographic systems. More particularly, the present invention relates to a method and apparatus for cryptographically processing data including a plurality of data segments.

BACKGROUND OF THE INVENTION

[0002] A number of encryption methods and cryptographic systems (cryptosystems) are currently used in various fields. For example, there are symmetric cryptosystems and asymmetric cryptosystems. The symmetric cryptography, which is also referred to as secret-key cryptography, uses a single key (secret key) to encrypt and decrypt information. Asymmetric cryptography, which is also referred to as public-key cryptography, uses a pair of keys: one (public key) to encrypt data, and the other (private key) to decrypt it. Currently available encryption algorithms include, for example, Data Encryption Standard (DES) which is a symmetric algorithm employing a block cipher with a single 56-bit key, triple DES which is a secure form of DES using a 168-bit key, International Data Encryption Algorithm (IDEA) which is a block-mode secret-key encryption algorithm using a 128-bit key, RC4 which is a widely-used symmetric key algorithm, the Advanced Encryption Standard (AES) which provides stronger encryption scheme with alternative three key lengths of 128 bits, 192 bits, or 256 bits, and the like.

[0003] Many companies employ a symmetric cryptosystem for their secure communications, using a predetermined encryption algorithm with the fixed secret-key such as the triple DES or AES. Due to the continuous evolution of computer-based technology, security methods that have seemed unbreakable are becoming inadequate, for example, the 56-bit key size of DES is no longer considered secure against brute force attacks. Using the same encryption algorithm and the same secret-key for communication over long time may increase the risk of brute force attacks on the

cryptosystem. However, replacing encryption algorithm and/or the secret-key in a once-implemented cryptosystem is typically very costly, since it requires some form of secure key exchange, in person, by courier, and the like, among all of the entities using the cryptosystem, and any change in the algorithm or secret key must also be synchronized among the entities. A fixed algorithm/key cryptosystem also lacks compatibility with other cryptosystems utilizing a different encryption algorithm and/or a different secret key.

[0004] Accordingly, it would be desirable to provide a cryptosystem which realizes secure communications and transactions which is less vulnerable to brute force and other attacks and also has high flexibility and compatibility.

BRIEF DESCRIPTION OF THE INVENTION

[0005] A method and apparatus cryptographically process data including a plurality of data segments. The cryptographic process includes (a) receiving a plurality of data segments, (b) selecting, for each data segment, a set of encryption information based on data contained in a predetermined portion of the data segment to be encrypted, and (c) encrypting each data segment using the set of encryption information selected for the data segment. At least one of an encryption algorithm, an encryption key, and an encryption parameter may be changed for each data segment based on the data contained in the predetermined portion. The predetermined portion may include a first predetermined portion for selecting a first set of encryption information, and a second predetermined portion for selecting a second set of encryption information, the encryption information including an encryption algorithm, an encryption key, and optionally an encryption parameter.

[0006] In accordance with one aspect of the present invention, a method for encrypting data includes (a) receiving a plurality of data segments, (b1) selecting, for each packet, a first set of encryption information based on data contained in a first predetermined portion of the data segment, (b2) selecting, for each packet, a second set of encryption information based on data contained in a second predetermined portion of the data segment, (c1) encrypting the second predetermined portion of each data segment

using the first set of encryption information selected for the data segment, (c2) encrypting the remaining portion of each data segment using the second encryption information selected for the data segment, and (d) generating an encrypted data segment for each of the original data segments, the encrypted data segment having a first predetermined portion, a second predetermined portion, and a remaining portion, the first predetermined portion containing the original data in the corresponding first predetermined portion of the original data segment, the second predetermined portion containing the encrypted data of the corresponding second predetermined portion of the original data segment, and the remaining portion containing the encrypted data of the corresponding remaining portion of the original data segment.

[0007] In accordance with one aspect of the present invention, the method for decrypting data includes (a) receiving an encrypted data including a plurality of encrypted data segments, each of the encrypted data segments having a first predetermined portion, a second predetermined portion, and a remaining portion, the first predetermined portion containing original data in a corresponding first predetermined portion of an original data segment, the second predetermined portion containing encrypted data of a corresponding second predetermined portion of the original data segment, and the remaining portion containing the encrypted data of the corresponding remaining portion of the original data segment, (b1) selecting, for each encrypted data segment, a first set of encryption information based on the original data contained in the first predetermine portion of the encrypted data segment, (c1) decrypting the encrypted data contained in the second predetermined portion of each encrypted data segment using the first set of encryption information selected for the encrypted data segment, (b2) selecting, for each encrypted data segment, a second set of encryption information based on the decrypted data of the second predetermined portion, (c2) decrypting the remaining portion of each encrypted data segment using the second set of encryption information selected for the encrypted data segment.

[0008] In accordance with one aspect of the invention, an apparatus for cryptographically processing data includes (a) means for receiving a plurality of data segments, (b) means for selecting, for each data segment, a set of encryption information

based on data contained in a predetermined portion of the data segment to be encrypted, and (c) means for encrypting each data segment using the set of encryption information selected for the data segment. The means for selecting may change at least one of an encryption algorithm, an encryption key, and an encryption parameter for each data segment based on the data contained in the predetermined portion.

[0009] In accordance with one aspect of the invention, the means for selecting includes (e) means for generating, for each data segment, a value from data contained in the predetermined portion of the data segment, and (f) means for selecting a set of encryption information associated with the generated value, the set of encryption information including an encryption algorithm, an encryption key, and optionally an encryption parameter. The means for generating a value may include means for hashing the data contained in the predetermined portion using a hash key.

[0010] In accordance with one aspect of the invention, the apparatus may further includes means for providing an encryption table containing an encryption type identifier, an encryption key for the encryption type, and an encryption parameter, for each entry associated with a generate value.

[0011] In accordance with one aspect of the invention, the predetermined portion includes a first predetermined portion for selecting a first set of encryption information, and a second predetermined portion for selecting a second set of encryption information. Each set of encryption information includes an encryption algorithm, an encryption key, and optionally an encryption parameter.

[0012] In accordance with one aspect of the invention, the apparatus may further include means for encrypting the second predetermined portion using the first set of encryption information, and means for encrypting the remaining portion of the data segment using the second set of encryption information.

[0013] In accordance with one aspect of the invention, the apparatus may further include means for generating an encrypted data segment for each of the original data segments, the encrypted data segment having a first predetermined portion, a second

predetermined portion, and a remaining portion, the first predetermined portion containing the original data in the corresponding first predetermined portion of the original data segment, the second predetermined portion containing the encrypted data of the corresponding second predetermined portion of the original data segment, and the remaining portion containing the encrypted data of the corresponding remaining portion of the original data segment.

[0014] In accordance with one aspect of the invention, the apparatus may further include means for transmitting a plurality of encrypted data segments as a stream of encrypted data. The apparatus may also include means for storing a plurality of encrypted data segments on a data storage device, each encrypted data segment corresponding to a respective data sector of the data storage device.

[0015] In accordance with one aspect of the invention, the apparatus may further include (a) means for receiving the encrypted data including a plurality of encrypted data segments, (b1) means for selecting, for each encrypted data segment, a first set of encryption information based on data contained in the first predetermine portion of the encrypted data segment, (c1) means for decrypting the encrypted data contained in the second predetermined portion of each encrypted data segment using the first set of encryption information selected for the encrypted data segment, (b2) selecting, for each encrypted data segment, a second set of encryption information based on the decrypted data of the second predetermined portion, and (c2) decrypting the remaining portion of each encrypted data segment using the second set of encryption information selected for the encrypted data segment.

[0016] In accordance with one aspect of the invention, the means for selecting the first encryption information may include means for generating a first value from the original data contained in the first predetermined portion of the encrypted data segment. The means for generating the first value may include means for hashing the data contained in the first predetermined portion using a first hash key.

[0017] In accordance with one aspect of the invention, means for selecting the second encryption information may include means for generating a second value from the decrypted data of the second predetermined portion of the encrypted data segment. The means for generating the second value may include means for hashing the decrypted data of the second predetermined portion using a second hash key.

[0018] In accordance with one aspect of the invention, the apparatus for decrypting data includes (a) means for receiving a plurality of encrypted data segments, each of the encrypted data segments having a predetermined portion, (b) means for selecting, for each encrypted data segment, a set of encryption information based on data contained in the predetermined portion of the encrypted data segment, and (c) means for decrypting each encrypted data segment using the encryption information selected for the encrypted data segment.

[0019] In accordance with one aspect of the invention, the means for selecting may include means for generating, for each encrypted data segment, a value from data contained in the predetermined portion of the encrypted data segment, and means for selecting a set of encryption information associated with the generated value, the set of encryption information including an encryption algorithm, an encryption key, and optionally an encryption parameter. The means for generating a value may include means for hashing the data contained in the predetermined portion using a hash key.

[0020] In accordance with one aspect of the invention, the apparatus may further include means for providing an encryption type identifier, an encryption key for the encryption type, and an encryption parameter associated with a generated value.

[0021] In accordance with one aspect of the invention, the predetermined portion may include a first predetermined portion for selecting a first set of encryption information, and a second predetermined portion for selecting a second set of encryption information. Each set of encryption information may include an encryption algorithm, an encryption key, and optionally an encryption parameter.

[0022] In accordance with one aspect of the invention, the first predetermined portion contains data for a first protocol layer, and the second predetermined portion contains data for a second protocol layer, wherein the first protocol layer is lower than the second protocol layer. The first predetermined portion may be an Internet Protocol (IP) header of the data packet. The second predetermined portion may be a selected portion of a data field, a Transmission Control Protocol (TCP) header, or a User Datagram Protocol (UDP) header of the data packet.

[0023] In accordance with one aspect of the invention, the first predetermined portion is a first selected portion in a sector in a data storage device, and the second predetermined portion is a second selected portion in the sector.

[0024] In accordance with one aspect of the invention, the data contained in the second predetermined portion of an encrypted data segment has been encrypted using the first set of encryption information, and the data contained in the remaining portion of the encrypted data segment has been encrypted using the second set of encryption information.

BRIEF DESCRIPTION OF THE DRAWINGS

[0025] The accompanying drawings, which are incorporated into and constitute a part of this specification, illustrate one or more embodiments of the present invention and, together with the detailed description, serve to explain the principles and implementations of the invention.

[0026] In the drawings:

FIG. 1A is a block diagram schematically illustrating an encryption part of an apparatus for encrypting/decrypting data in accordance with one embodiment of the present invention.

FIG. 1B is a block diagram schematically illustrating an decryption part of an apparatus for encrypting/decrypting data in accordance with one embodiment of the present invention.

FIG. 2 is a diagram schematically illustrating an example of the encryption table

in accordance with one embodiment of the present invention.

FIG. 3 is a process flow diagram schematically illustrating a method for encrypting/decrypting data in accordance with one embodiment of the present invention.

FIG. 4 is a diagram schematically illustrating an example of a data packet in which the first predetermined portion is an Internet Protocol (IP) header, and the second predetermined portion is a Transmission Control Protocol (TCP) header.

FIG. 5 is a diagram schematically illustrating an example of a data packet in which the first predetermined portion is an Internet Protocol (IP) header, and the second predetermined portion is a User Datagram Protocol (UDP) header.

FIG. 6 is a diagram schematically illustrating an example of a data packet in which the first predetermined portion is an Internet Protocol (IP) header, and the second predetermined portion is a selected portion of a data field.

FIG. 7 is a diagram schematically illustrating an example of the first and second predetermined portions in a sector of a data storage device.

FIG. 8 is a diagram schematically illustrating an example of the first and second predetermined portions in a data segment stored in a memory card in which the data segment corresponds to data stored in each address.

FIG. 9 is a process flow diagram schematically illustrating a method for encrypting data in accordance with one embodiment of the present invention, in which the predetermined portion includes a first predetermined portion and a second predetermined portion.

FIG. 10 is a diagram schematically illustrating an example of encrypting a data packet using the method shown in FIG. 9.

FIG. 11 is a process flow diagram schematically illustrating a method for decrypting encrypted data in accordance with one embodiment of the present invention, in which the predetermined portion includes a first predetermined portion and a second predetermined portion.

FIG. 12 is a diagram schematically illustrating an example of decrypting a data packet using the method shown in FIG. 11.

FIG. 13 is a block diagram schematically illustrating a data encryptor/decryptor in accordance with one embodiment of the present invention.

FIG. 14 is a diagram schematically illustrating an example of application of the

encryption/decryption apparatus to secure communications via the Internet in accordance with one embodiment of the present invention.

DETAILED DESCRIPTION

[0027] Embodiments of the present invention are described herein in the context of a method and apparatus for encrypting and decrypting data including a plurality of data segments. Those of ordinary skill in the art will realize that the following detailed description of the present invention is illustrative only and is not intended to be in any way limiting. Other embodiments of the present invention will readily suggest themselves to such skilled persons having the benefit of this disclosure. Reference will now be made in detail to implementations of the present invention as illustrated in the accompanying drawings. The same reference indicators will be used throughout the drawings and the following detailed description to refer to the same or like parts.

[0028] In the interest of clarity, not all of the routine features of the implementations described herein are shown and described. It will, of course, be appreciated that in the development of any such actual implementation, numerous implementation-specific decisions must be made in order to achieve the developer's specific goals, such as compliance with application- and business-related constraints, and that these specific goals will vary from one implementation to another and from one developer to another. Moreover, it will be appreciated that such a development effort might be complex and time-consuming, but would nevertheless be a routine undertaking of engineering for those of ordinary skill in the art having the benefit of this disclosure.

[0029] In accordance with one embodiment of the present invention, the components, process steps, and/or data structures may be implemented using various types of hardwired devices, field programmable logic devices (FPLDs), including field programmable gate arrays (FPGAs) and complex programmable logic devices (CPLDs), application specific integrated circuits (ASICs), or the like, may also be used without departing from the scope and spirit of the inventive concepts disclosed herein.

[0030] In the context of the present invention, the term "network" includes local area networks (LANs), wide area networks (WANs), the Internet, cable television systems, telephone systems, wireless telecommunications systems, fiber optic networks, ATM networks, frame relay networks, satellite communications systems, and the like. Such networks are well known in the art and consequently are not further described here

[0031] FIG. 1A schematically illustrates an apparatus **10** for encrypting/decrypting data in accordance with one embodiment of the present invention. As shown in FIG. 1A, the apparatus **10** includes an input buffer **12**, an encryption module **14**, a controller **16** coupled to the input buffer **12** and the encryption module **14**, and an output buffer **18** coupled to the controller **16** and the encryption module **14**. The input buffer **12** is adapted to receive data including a plurality of data segments. For example, such data may be a data stream including a plurality of data packets. The data segments may also be read from corresponding sectors of a recording medium or data storage device such as a hard disk, CD ROM, DVD, memory card, and the like. The encryption module **14** is adapted to encrypt each data segment. The output buffer **18** buffers the encrypted data segments from the encryption module **14**, and outputs encrypted data including a plurality of encrypted data segments.

[0032] For example, as shown in FIG. 1A, the apparatus **10** may be used between a universal serial bus (USB) port **11** and an Ethernet port **13**, in such a case where a host computer communicates via a LAN. The apparatus **10** can also be used for secure communications via WAN, the Internet, wireless network, and the like. Furthermore, the apparatus **10** may be used with a small computer system interface (SCSI), an intelligent/integrated drive electronics (IDE) interface, an enhanced IDE interface, and the like, to store secure data in mass storage devices. The apparatus may also be used for the other type of digital data transfer.

[0033] The controller **16** is adapted to select a set of encryption information for each data segment based on data contained in a predetermined portion of the data segment to be encrypted. For example, the encryption information includes an encryption algorithm, an encryption key, and an encryption parameter such as an initial vector. The

encryption parameter may be used to set or initialize the encryption process to a specific state. Since the encryption information is selected based on data in a specific portion of the data segment to be encrypted, typically, at least one of the encryption algorithm, the encryption key, and the encryption parameter is changed for each data segment. In other words, the encryption information is "self-determined" for each data segment using the data contained in the data segment itself. The predetermined portion of the data segment may be a header of each data packet, a selected portion of the data field of the data packet, for example, a specific length of data starting at a predetermined number of bytes from the beginning of the data field. The predetermined portion may be a selected portion of a sector in a data storage device, a sector number or address field of each sector in a data storage device, and the like.

[0034] The encryption module **14** includes a plurality of encryption engines **20** (**20a, 20b, 20c**,...), each corresponding to an encryption algorithm to be selected by the controller **16**. The encryption module **14** may further include a data buffer **22** coupled to each of the plurality of encryption engines **20.**

[0035] In accordance with one embodiment of the present invention, as shown in FIG. 1A, the controller **16** includes a data selector **24**, an encryption selector **26** coupled with the data selector **24**, and an encryption controller **28**. The data selector **24** is adapted to select the predetermined portion from each data segment. The encryption selector **26** is adapted to select a set of encryption information in accordance with data contained in the predetermined portion selected by the data selector **24**. The set of encryption information includes, for example, an encryption algorithm, an encryption key, and optionally an encryption parameter. The encryption controller **28** is adapted to select and activate one of the encryption engines **20** based on the encryption information. For example, if an encryption algorithm A is selected by the encryption selector **26**, the encryption controller **28** selects a corresponding encryption engine (A) **20a** and activates or initializes the encryption engine **20a** using the encryption parameters. The data is encrypted by the encryption engine **20a** using the selected key. It should be noted that a different key and/or a different encryption parameter yield different encrypted data even if the same encryption algorithm and the thus same encryption engine are used.

[0036] In accordance with one embodiment of the present invention, the controller 16 further includes a value generator **30** coupled to the data selector **24.** The value generator is adapted to generate a value from the data contained in the predetermined portion. For example, the value generator **30** may include a hash function and hash the data using a hash key to produce the value. The hash key may be preinstalled in the value generator **30**, or may be selected when the controller 16 is first programmed.

[0037] In accordance with one embodiment of the present invention, the encryption controller **26** includes an encryption table **32**. The encryption table **32** contains an encryption type identifier, an encryption key for the encryption type, and an encryption parameter such as an initial vector specifying an initial encryption state of the encryption engine, for each entry associated with a value generated by the value generator **30**. FIG. 2 schematically illustrates an example of the encryption table **32**. As shown in FIG. 2, each entry of the encryption table **32** has an index corresponding to the generated value, for example, a hash value, and a corresponding set of an encryption algorithm (encryption type), a key for the encryption algorithm, and an initial vector (encryption parameter). The number of the entries depends on the value generated from the predetermined portion. In one embodiment of the present invention, an encryption table has about 1000 entries. Typically, a different index value is derived from the predetermined portion of a different data segment, and thus each data segment is encrypted using different encryption information.

[0038] The above description is with respect to the encryption part of the apparatus 10. FIG. 1B schematically illustrates a corresponding decryption part **10'** of the apparatus **10** in accordance with one embodiment of the present invention. As shown in FIG. 1B, the decryption part **10'** can be constructed symmetrically to the encryption part (FIG. 1A) of the apparatus **10**, including decryption engines **20a', 20b'**, and **20c'** in place of the encryption engines **20a, 20b**, and **20c**, as is well understood by one of ordinary skill in the art without further explanation.

[0039] FIG. 3 schematically illustrates a method for encrypting/decrypting data in accordance with one embodiment of the present invention. The method may be performed by the encryption/decryption apparatus **10**. A plurality of data segments are received, for example, by receiving a data stream including a plurality of data packets, or reading from a data storage device including a plurality of data sectors or addresses. The received data segments may be buffered by an input buffer. The data segments are encrypted segment by segment. As shown in FIG. 3, each data segment is received **(100),** and a predetermined portion of each data segment is selected **(102),** and a set of encryption information is selected based on data contained in the predetermined portion of the data segment to be encrypted **(104).** The data segment is encrypted using the selected set of encryption information **(106).** The next data segment is processed in the same manner until all data segments in the input buffer are processed **(108).** The set of encryption information may include an encryption algorithm, an encryption key, and optionally an encryption parameter, as described above, ant typically at least one of the encryption algorithm, the encryption key, and the encryption parameter is changed for each data segment based the data contained in the predetermined portion.

[0040] As discussed above, in selecting the encryption information, a value (such as a hash value) may be generated from the data contained in the predetermined portion of the data segment, and the set of encryption information may be selected using the generated value. The set of encryption information may be provided in a form of an encryption table such as the encryption table **32** (FIG. 2) described above.

[0041] In accordance with one embodiment of the present invention, the predetermined portion includes a first predetermined portion and a second predetermined portion. In the case where the data segment is a data packet, the first predetermined portion may contain data for a first protocol layer, and the second predetermined portion may contain data for a second protocol layer which is higher than the first protocol layer in the protocol hierarchy. The first protocol layer may be the network layer (or the Internet layer), and the second protocol layer may be the Transport layer.

[0042] FIG. 4 schematically illustrates an example of a data packet **34** in which the first predetermined portion is an Internet Protocol (IP) header **36**, and the second predetermined portion is a Transmission Control Protocol (TCP) header **38** of the data packet **34**. FIG. 5 schematically illustrates an example of a data packet **40** in which the first predetermined portion is an Internet Protocol (IP) header **36**, and the second predetermined portion is a User Datagram Protocol (UDP) header **42** of the data packet **40**. It should be noted that although the IP header **36**, the TCP header **38**, and the subsequent TCP data field **44** are illustrated separately in FIG. 4, they are contiguous in the data packet **34**. Similarly, although the IP header **36**, the UDP header **38**, and the subsequent UDP data field **46** are illustrated separately in FIG. 5, they are contiguous in the data packet **40**. In addition, the information illustrated in each header is by way of example, and not limiting in any way. All of the information in the header may be used to derive a (hash) value, or some part of the information may be selected to generate a value.

[0043] In accordance with one embodiment of the present invention, the second predetermined portion is not limited to a TCP or UDP header, but may be selected from a data field. FIG. 6 schematically illustrates an example of a data packet **48** in which the first predetermined portion is an Internet Protocol (IP) header **36**, and the second predetermined portion is a selected portion **52** (**52a**, **52b**, and **52c**) of a data field **50** of the data packet **48**. As shown in FIG. 6, the selected portion **52** may be divided and distributed in the data field **50**, and specified by a predetermined number of bytes from the beginning of the data field **50** and a predetermined data length. One single portion may be selected.

[0044] In accordance with one embodiment of the present invention, the data segments may be sectors in a data storage device such as a hard disk, CD ROM, DVD, memory card, or other mass storage device. In this case, the first predetermined portion is a first selected portion in a sector in a data storage device, and the second predetermined portion is a second selected portion in the sector. FIG. 7 schematically illustrates such an example. In FIG. 7, the first predetermined portion is a first selected portion **56** in a sector **54** in a data storage device, and the second predetermined portion

is a second selected portion **58 (58a, 58b)** in the sector **54**. FIG. 8 schematically illustrates an example of a memory card in which the data segment corresponds to data stored in each address. In such a case, the data may be encrypted address by address, and the first predetermined portion is a first selected portion **62 (62a, 63b)** in a memory address **60**, and the second predetermined portion is a second selected portion 64 in the address **60**. As shown in FIGS. 7 and 8, the first and/or second predetermined portion may be divided and distributed in the sector or data in the memory address, or may be a single portion.

[0045] FIG. 9 schematically illustrates a method for encrypting data in accordance with one embodiment of the present invention, in which the predetermined portion includes a first predetermined portion and a second predetermined portion, as described above. FIG. 10 schematically illustrates an example of encrypting a data packet **70** using the method shown in FIG. 9, where the data packet **70** includes a first predetermined portion **72** (such as an IP header) and a second predetermined portion **74** (such as a TCP header or a selected portion of the data field).

[0046] As shown in FIG. 9, for each data segment received **(110),** the first predetermined portion and the second predetermined portion are selected **(112, 114).** Also referring to FIG. 10, the first encryption information **78** is selected based on the data contained in the first predetermined portion **72 (116).** As discussed above, this selection **116** may include, for example, deriving a hash value from the first predetermined portion **72** and selecting the first encryption information using an encryption table associating the hash value with a respective set of encryption information. Similarly, the second encryption information **79** is selected based on the data contained in the second predetermined portion **74 (118).** This selection **118** may also include, for example, deriving a hash value from the second predetermined portion **74** and selecting the second encryption information using an encryption table associating the hash value with a respective set of encryption information. A respective hash key and a respective encryption table may be provided for each of the selection process **116** and **118**. For example, the controller **16** of the encryption/decryption apparatus **10** (FIG. 1) may include a first set of the hash key and the encryption table for the first

predetermined portion, and a second set of the hash key and the encryption table for the second predetermined portion.

[0047] Then, the second predetermined portion **74** is encrypted using the first encryption information **78 (120),** and the remaining portion of the data segment **76** is encrypted using the second encryption information **79 (122).** The remaining portion **76** is all of the remaining data in the data segment other than the first and second predetermined portions. As shown in FIG. 10, the first predetermined portion **82** containing the original data (also referred to as "plaintext"), the second predetermined portion **84** containing encrypted data (also referred to as "ciphertext"), and the remaining portion **86** containing encrypted data are combined to generate an encrypted data segment (packet) **80** corresponding to the original data segment (packet) **70 (124).** For example, referring to FIG. 1, the second predetermined portion may be encrypted using the encryption engine **20a**, and the remaining portion may be encrypted using the encryption engine **20b**, and the respective encrypted data are combined with the first predetermined portion into the encrypted data segment in the data buffer **22**, and sent to the output buffer **18**.

[0048] The processes **110** through **124** are performed until all of the data segments are encrypted **(126).** It should be noted that the selection and encryption processes are controlled such that the second encryption information **79** is selected before the data contained in the second predetermined portion **74** is encrypted, and the plaintext data for the first predetermined portion **84**, the ciphertext for the second predetermined portion **84**, and the ciphertext for the remaining portion 86 are sent to the data buffer **22** in this order.

[0049] The encrypted data segments may be transmitted as an encrypted data stream for secure data communication, or may be stored on a data storage device to prevent, for example, sensitive or protected information from being read by an unauthorized person.

[0050] FIG. 11 schematically illustrates a method for decrypting encrypted data in accordance with one embodiment of the present invention, in which the predetermined

portion includes a first predetermined portion and a second predetermined portion. FIG. 12 schematically illustrates an example of decrypting an encrypted data packet **80** using the method shown in FIG. 11, where the encrypted data packet **80** includes a first predetermined portion **82** (such as an IP header) and a second predetermined portion **84** (such as a TCP header or a selected portion of the data field). As described above, the first predetermined portion **82** contains plaintext, and the second predetermined portion and the remaining portion **86** contain ciphertext.

[0051] As shown in FIG. 11, for each encrypted data segment received **(130)**, the first predetermined portion and the second predetermined portion are selected **(132, 134)**. The encrypted data segments may be received as an encrypted data stream in a secure communication, or may be read from a data storage device. Also referring to FIG. 12, the first encryption information **88** is selected based on the data contained in the first predetermined portion **82 (136)**. Similarly to the encryption process discussed above, this selection **136** may include, for example, deriving a hash value from the first predetermined portion **82** and selecting the first encryption information using an encryption table associating the hash value with a respective set of encryption information. Since the first predetermined portion contains the plaintext, the first encryption information is the same as the original data segment.

[0052] Then, the second predetermined portion **84**, which contains the ciphertext, is decrypted using the first encryption information **88 (138)**. The second encryption information **89** is selected based on the decrypted data **85** contained in the second predetermined portion **84 (140)**. This selection **138** may also include, for example, deriving a hash value from the decrypted data **85** and selecting the second encryption information **89** using an encryption table associating the hash value with a respective set of encryption information. A respective hash key and a respective encryption table may be provided for each of the selection process **136** and **138**.

[0053] Then, the remaining portion **86** of the data segment is decrypted using the second encryption information **89 (142)**. The remaining portion **86** is all of the remaining data of the data segment other than the first and second predetermined

portions. The first predetermined portion **92**, the second predetermined portion **94**, and the remaining portion **96** are combined to generate an decrypted data segment (packet) **90** which is the same as the original data segment (packet) **70 (144)**. The processes **130** through **144** are performed until all of the encrypted data segments are decrypted **(146).**

[0054] FIG. 13 schematically illustrates a data encryptor/decryptor **150** in accordance with one embodiment of the present invention. As shown in FIG. 13, the data encryptor/decryptor includes a transmitting portion **152** and a receiving portion **162.** The transmitting portion **152** includes a first timing analyzer **154**, an encryption module (T) **156**, and a first data buffer **158.** Similarly, the receiving portion **162** includes a second timing analyzer **164**, a decryption module (R) **166**, and a second data buffer **168.** The encryption module **156** may be the encryption part of the encryption/decryption apparatus **10** (the encryption module **14** and the controller **16**) described above, and the decryption module **166** may be the encryption part **10'** of the encryption/decryption apparatus **10** described above. In the transmitting portion, for example, the input buffer **12** (in FIG. 1A) may be integrated within the timing analyzer **154** in accordance with a specific implementation. The output buffer **18** (in FIG. 1A) may also be integrated within the data buffer **158** in accordance with a specific implementation. The same applies to the receiving portion **154.**

[0055] Since the data encryptor/decryptor **150** typically transmits and receives a data stream (Tx and Rx), the timing analyzers **154** and **164** synchronize the encryption/decryption processes for the corresponding data stream such that encrypted/decrypted data are properly combined into respective encrypted/decrypted data segments (data packets) and sent to and output from the data buffers **158** and **168,** respectively.

[0056] In accordance with one embodiment of the present invention, the data encryptor/decryptor **150** (and the encryption/decryption apparatus **10**) can be implemented in a form of a plug-in card for a computer. Since all of the necessary components for encryption/decryption are provided in the data encryptor/decryptor (encryption/decryption card), the user/computer does not have to install any specific

software program for encryption/decryption so long as the computer can use the encryption/decryption card (i.e., port-compatible). By simply transmitting or storing data via the encryption/decryption card, the data is automatically encrypted and thus securely transmitted through a network or securely stored in a storage device. The same encryption/decryption card can be used to receive securely transmitted data or read the securely stored data.

[0057] To receive or read the encrypted data, the same encryption/decryption card or apparatus must be used to decrypt the encrypted data. The "same" means that the card or apparatus is capable of selecting the same predetermined first and second portions from the data segments and selecting/deriving the same first and second encryption information if the data contained in the predetermined portion is the same. Typically, for example, the corresponding (communicating) encryption/decryption cards have the identical hash keys and the identical encryption tables.

[0058] In accordance with one embodiment of the present invention, the encryption/decryption module part **170** (in FIG.13) can be customized according to the user's request at the time of manufacturing or initial programming. For example, since the encryption/decryption card can be implemented in field programmable logic devices (FPLDs), such as FPGAs and CPLDs, the encryption/decryption card or apparatus can be programmed in accordance with the user's specification (e.g., the degree of security, transmission speed, required protocol or standard, specific storage medium and/or format to be used, etc.) with specific settings of the hash keys and encryption tables (encryption information).

[0059] In addition, the user and the computer do not have to know the settings, and the settings are not accessible to the user and computer, such information cannot be stolen from the user or the computer to "crack the code." Furthermore, the encryption algorithm, the encryption key, and optionally the encryption parameter are practically changed for every data segment, and which algorithm, key, and parameter to be used are only "known" to the data segment itself to be encrypted. Since the encryption algorithm, key, and/or parameter are automatically changed based on certain data contained in the

data segment itself, synchronization between the transmitting side and the receiving side is unnecessary.

[0060] FIG. 14 schematically illustrates an example of application of the present invention to secure communications via the Internet. As shown in FIG. 14, users **180. 182, 184** can use respective encryption/decryption apparatuses **190, 192,** and **194** in accordance with one embodiment of the present invention. The encryption/decryption apparatuses **190, 192**, and **194** may be the encryption/decryption apparatus **10** or encryptor/decryptor **150** as described above. All of the encryption/decryption apparatuses **190, 192**, and **194** are programmed identically and provided with the same settings, for example, the same hash keys and encryption tables. As shown in FIG. 14, the encryption/decryption apparatus may be used by more than one computers **184** and **186.** For example, the encryption/decryption apparatus **194** may be used with a hub within a LAN such that all data transmissions from the computers or host connected to the hub are encrypted.

[0061] In accordance with one embodiment of the present invention, since the IP header of each data packet is not encrypted, the encryption/decryption scheme of one embodiment of the present invention does not affect routing or switching of the data packets via the Internet or other networks (i.e., operations in the network protocol layer). In addition, in the case where some routers may possibly look into a packet field other than IP header in their routing operation, the first predetermined portion can be selected such that it includes the IP header and such portion of the data field to be used by the routers.

[0062] In accordance with one embodiment of the present invention, as described above, each data segment is encrypted using the two-level encryption. That is, the data segment other than the first and second predetermined portions is encrypted using the information contained in the second predetermined portion. Then, the second predetermined portion is encrypted using the information contained in the first predetermined portion. Thus, although the first predetermined portion contains plaintext, the second predetermined portion containing encrypted data (ciphertext) provides

additional level of security, since the second predetermined portion and the remaining portion are typically encrypted by a different encryption algorithm, a different encryption key, and/or a different encryption parameter. In addition, since the encryption algorithm, the encryption key, and/or the encryption parameter are changed for every data segment, it is practically impossible to clack the code by a hacker.

[0063] While embodiments and applications of this invention have been shown and described, it would be apparent to those skilled in the art having the benefit of this disclosure that many more modifications than mentioned above are possible without departing from the inventive concepts herein. The invention, therefore, is not to be restricted except in the spirit of the appended claims.